A Novel Approach for Detecting Black Hole Attack in MANET

Isha Shingari
M.TechComputer Science Engineering
MITS Laxmangarh

Sourabh Singh Verma
Asst. Professor, Computer Science Department
MITS Laxmangarh

ABSTRACT

The communication in Mobile Adhoc Networks play a vital role in situations like natural calamities or military operations, but due to the dynamic nature of the adhoc networks, it is very important to take care of the security issues, one of the major security issues is the detection of compromised node. The calculation of trust values on the neighboring nodes can significantly solve this problem. This paper presents the calculation of trust values based on the threshold value, if trust value of a node goes beyond the predefined threshold, it is considered to be malicious. The trust value of a node is calculated by taking average of all the trust values for the node. The proposed scheme will be able to detect and isolate the compromised node from the network**.**

General terms
Security protocol, black hole attack, trust averaging

Keywords
MANET, threshold trust, trust calculation, trust

1. INTRODUCTION

Mobile Adhoc Network is a dynamic, self-configuring network which consists of the nodes working in an adhoc manner without any predetermined topology. A Mobile AdhocNetwork(MANET) is more susceptible to security attacks than the wired medium. A compromised node in the network is one such issue that can compromise the quality of service and reliability of data delivered by the network. It is very crucial to keep a check on it. Calculation of trust in the network provides a beneficial solution to the problem, but it is a very challenging task due to dynamic nature of the network [1].

MANETs lack a centralized system, without being dependent on the central authority, every node in the network has to evaluate the trust of other nodes by its own experience and also by the recommendation of other neighborhood nodes. The trust can be quantified if it is calculated within a range because within a certain range a threshold trust value for ongoing task can be reasonably defined [2]. The threshold trust values marks a limit of trust which a node has to achieve to remain trusted. A threshold value of 0.3 is defined and the nodes having trust values less than that are considered untrusted or compromised.

Consider a case where a node 'X' is transferring information packets to two nodes, node 'Y' and 'Z', the trust value for node 'Y' is 0.2 and node 'Z' is 0.8. In this case the node is trustworthy for one node whereas compromised for the other. If any one of the values is taken, The averaging of trust values can definitely give the solution, 0.5 will be the final trust value which is greater than the threshold value. The fuzzy logic provides the ability to handle the imprecision and uncertainty effectively [3], the fuzzy logic based algorithm is applied over the calculated trust values of the nodes. These values are taken as the input and the algorithm classify the nodes as trustworthy or compromised.There has to be some optimized path calculated for routing the nodes in MANET, after getting the trusted nodes and bypassing the compromised nodes in the network, it becomes crucial to route the according to maximum trust values. [4].

The major contribution to the paper are taking the threshold trust value, calculating the trust, averaging the trust and determining the nodes are trusted or compromised. These are well explained in the following sections. In section II, the different trust accounting measures for MANET are mentioned. In section III, IV, V the trust calculation, trust model and trust evaluation approach are mentioned respectively. The section VI consists of the proposed work; finally the work is summarized and the future work is explained in the conclusion section.

2. RELATED WORK

The importance of trust is well studied in various research domains like economics, law, political science, management and psychology. In information technology, the trust evaluation and trust metrics are mainly defined for the access control [5], electronic commerce [6, 7] and public key authentication [8-12]. All these schemes are proposed for the static networks and cannot be applied directly in case of MANETs which are dynamic in nature.

An authentication service against the dishonest nodes in Mobile Adhoc Network was proposed by Ngai, Lyu and Chin [5]. It was calculated by the application of Beth, Borcherding and Klein's trust evaluation model introduced in [6]. In [6] this approach there are two measures to calculate the trust: direct trust and recommended trust.

Each of the above trust can be expressed and computed into a real number which ranges between 0 and 1. However, this approach was designed for the open static networks. Its trust evaluation between two end nodes is on the basis of direct experience or recommendations through other nodes, but this is not calculated at the same time for the two end nodes. Therefore, there is no relationship defined which can balance the direct and recommendation trust in the approach.

A pure trust model to establish trust in MANETs was proposed by Pirzada and McDonald in [7,13]. The computation of trust is on the basis of monitoring the data

delivery inside the network. The trust value id is calculated in the range from -1 to +1. The negative value for trust can occur as the result of more failures than the success for varies events occurring in the network. This model is designed for the routing in MANETs. The trust evaluation in Mobile Adhoc Network depends upon the direct data communication of each node in MANETs. The pre-existing knowledge or recommendation from other nodes is not considered. Yan, Zhang and Virtanen in [14] proposed a trust model which was for the secure routing evaluation in MANET. The trust evaluation matrix was calculated, which was on the basis of the statistic data collected during the network communication. A linear function is used to link the statistic fields together to compute the trust value about a certain node. No boundary evaluation is defined in the approach. It becomes a difficult task to define the threshold value for the on-going tasks. A pair-wise trust evaluation scheme in MANETs was proposed by Virendra, et al. in [15]. The trust of the target node is calculated while implementing the self evaluation on the target node. The trust values of other nodes in the network on the target node are also considered. All the trust values are evaluated by the node monitoring on data delivery inside the network. In order to compute the self evaluation, a statistic function is mentioned. This function is not explicitly presented.

The source based routing protocol explained in [16] makes use in AODV; compromised nodes are detected and isolated from the network by dynamically updating the trust values. These trust values classify the nodes as compromised or trustworthy. The trust based approach explained in [17] presents a collaborative approach in mitigating blackhole attacks in AODV protocol in MANET. It uses the concept of threshold value and the trust values below the threshold value are considered to be malicious.

The opinion based trust model in [4] evaluates trust at different levels. The nodes behave in a promiscuous manner. Each node determines the trustworthiness of other nodes on account of behavior observed. It calculates the direct trust and the indirect trust obtained by the opinion of other nodes. Some of the nodes are made supervisor nodes. The supervisor nodes may behave maliciously with the course of time. Security in MANET is a major issue, it has to be handled very carefully. MANETs lack a centralized support and the topology is also continuously changing and the presence of compromised node makes the situation more vulnerable. There has to be a proper mechanism which can isolate the compromised node completely, a novel approach of trust calculation has been proposed in which evaluating the trust for every node will limit the number of broadcasted RREQ. The approach is explained in the following sections.

3. TRUST EVALUATION

The trust evaluation in MANET is a demanding task. MANETs have the different network properties. The trust is calculated on the basis of the previous individual experiences of the node and on the recommendations of its neighbors. The ability of assessing the trust level of its neighbors brings in several advantages. Firstly, a node can detect and isolate the malicious behaviors which avoid the relaying packets to malicious neighbors. Secondly, the cooperation is stimulated by selecting the neighbors with the higher trust values [3][4].

3.1 Trust Calculation

(a) Direct trust calculation: There is a directed trust between node 'j 'and node 'i'.

DTV=(1-
(DP/FP))……..…….(1)[17]

The direct trust value shows the value of the immediate value of trust calculated for the particular node. It monitors the behavior of the node. The number of Dropped Packets (DP), Forwarded Packets(FP) and delayed packed are analyzed for the calculation of the direct trust value for the node.

(b) Recommended trust value: The recommended trust value calculates the amount of recommended trust for the neighboring node. Or in the simpler terms, it can be said that the neighboring trust values are calculated.

Intercluster trust calculation:

$ITR_{ij} = \Sigma (DTR_{hi} * DTR_{ij}) / \Sigma (DTR_{hi} DTR_{hi} > H, i \neq j$….(2)

The value of i varies from 1 to t. DTR_{hi} is aggregation weight and DTR is Direct Trust Recommendations**.**

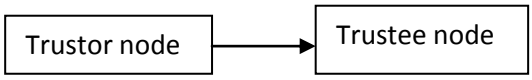

Figure: 1 Direct Trust

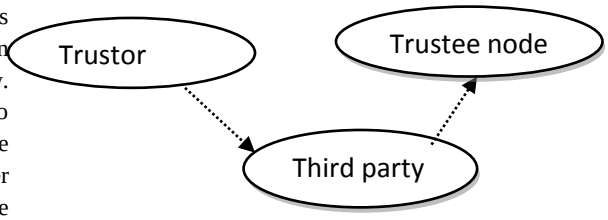

Figure: 2 Recommended Trust

4. TRUST MODEL FOR MANET

Trust is a vital factor for the deployment and design of the security systems. In MANET, the trust evaluation is applied for the access control, trust routing and node authentication. By the evaluation of the trust of the related nodes, the system security is enhances and it thereby improves the routing performance in MANETs. For defining the suitable trust evaluation for MANET, there are various issues which need to be taken into consideration.

For quantifying the trust, it would be helpful, if the deployed function can be used to evaluate the trust value in a certain range, because if the trust values are calculated in a particular range the threshold values can be defined. Secondly, the MANETs are dynamic due to the mobile nature of the nodes. The dynamic nature of MANETs suggests that the nodes within the network may be instantaneous or communicative in nature. The other factor is that the trust is evaluated according to the human psychology and its consequent behavior. Finally, the trust model should be suitable to the different situations of the system. The nodes may be free to join or leave the system [3][18].

5. TRUST EVALUATION APPROACH

5.1 AODV routing protocol

AODV (AdhocOn Demand Distance Vector) starts the path identification phase to destination when there is a need for data transmission. AODV uses a local broad cast message called as "hello"message, which provides the local connectivity information to the node. AODV performs two main operations 1) path discovery and 2) path maintenance. The path discovery process will be initiated when the source nodes want to communicate with the destination node, the source node will send a RREQ (Route Request) to its neighboring nodes. The neighboring nodes after receiving the RREQ will check the destination Id of the RREQ, if the destination Id matches with the node Id of the receiving node; it will send a RREP (Route Reply) to the source node[18].

5.2 Introduction to trust based protocol

Each node in a MANET moves independently in any direction, thus the wireless nodes try to communicate in the destination node by using the intermediate nodes. In such kinds of situations, MANET is vulnerable to both internal and external attacks caused by malicious nodes present in the network. The motive of the approach is to provide the security to Ad hoc On-demand Distance Vector (AODV) protocol, which helps AODV in detecting the compromised nodes. This proposed approach is able to detect the compromised nodes and isolates it from the network. The reliability of the trusted AODV routing protocol is evaluated by implementing black hole attack and the performance is calculated in terms of metrics like packet delivery ratio, throughput and average end to end delay.

Intermediate nodes may drop the packets due to malicious attacks such as black hole, gray hole etc or poor wireless network quality and heavy congestion in the network. Trust evaluation in routing procedure has become a remark of a sender after it gets a forwarding service of another node.The control messages play a role in determining the path from source to destination in-order to transfer data among them. In AODV, if the control packet RREQ which has been processed by a node with same sequence number already appears then the particular RREQ will be discarded considering it as a duplicate control packet.

5.3Assigning the trust values

Initially all the nodes in the network will be assigned with a trust value (T). Further the trust value of a node will increase if it is a benevolent node (T+1) and the trust value of a node willdecrease if it is a malevolent node (T-1). The working principle of the proposed methodology is as follows:

- Consider two nodes *i* and *j*.
- If node 'i'wants to transmit a packet to the destination node n,
- The node 'i' sends a route request to the neighboring node 'j',
- Node 'j'after receiving the control packet from node 'i'and check the destination id, if the destination id does not match with the control packet sent by node 'i', node 'j'broadcasts the route request to its neighboring nodes. The above action will occur only if node 'j'is a benevolent one.

5.4 Making decision by deciding the threshold value

Initially all the nodes in the network will be assigned with a trust value (T). Further the trust value of a node will increase if it is a benevolent node (T+1) and the trust value of a node will decrease if it is a malevolent node (T-1).

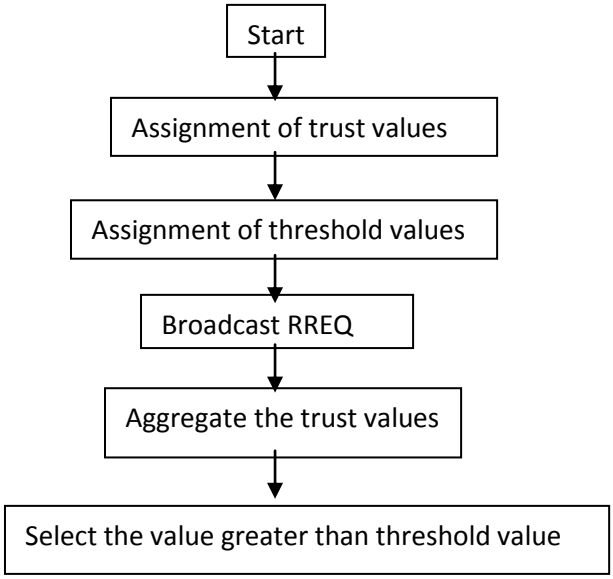

Figure3: Decision of the threshold value

6. PROPOSED TECHNIQUE

6.1 Behavior

This accounts for the behavior of the nodes. This announces the node to be trust worthy or compromised. The more trust situations node undergoes, more trustworthy it becomes. It is judged that the modification of the packet information has been done or the packet has been dropped.

6.2 Classifier

It classifies the trust values of the node. The values range from 0 to1. The values ranging below 0.3 are considered to be non-trustworthy. The values ranging between 0.3 and 0.5 are under the suspect count list and above 0.5 are the trusted nodes. The trust is calculated as:

T= 1-D/F…….(3)

T = trust value

D= number of packets dropped by a node, which are actually to be forwarded.

F= number of packets forwarded to that node, which are actually further forwarded.

The individual trust values are calculated, the values less than the threshold (0.3) are broadcasted throughout the network.

6.3 Aggregating the trust values

Consider the following scenario

There is a network consisting of 5 nodes namely node ‘A’,’ B’, ‘X’,’Y’ and ‘Z’. Here, as the figure shows, ‘Z’ is connected to ‘A’, ‘Y’ and ‘Z’. Node ‘Y’ and node ‘X’ want to send the information to ‘A’through node ‘Z’. The trust value of the node is calculated by (3). The trust value of node ‘Z’ for node ‘Y’ comes out to be 0.2. The threshold trust value is 0.3 for the network. As a result, the trust value of node ‘Z’ for node ‘Y’ is less than the threshold. The node ‘Y’ considers the node ‘Z’ as malicious. So, node ‘Y’ will broadcast the trust value i.e less than 0.3 to all its neighbours.(A node will only broadcast trust value if it is less than 0.3) .

The node ‘Y’ will look for other paths in the network and omit ‘Z’ entry from routing table. After receiving the trust value from node ‘Y’ for node ‘Z’, the node ‘X’s, averaged trust value (earlier 0.8) will become 0.5. The value 0.5 is greater than the threshold trust value. The node z is trustworthy for node ‘X’. In this case, the node ‘Z’ is malicious for node ‘Y’ but trustworthy for node ‘X’, the node ‘Y’ would have broadcasted this information throughout the network, this would increment the number of RREQ s. A solution to this problem is provided by taking the averaged trust values, the information could be passed onto the trusted node. The averaged value will prevent the node ‘x’ from discarding the node z as non-trusted path and broadcasting the information.

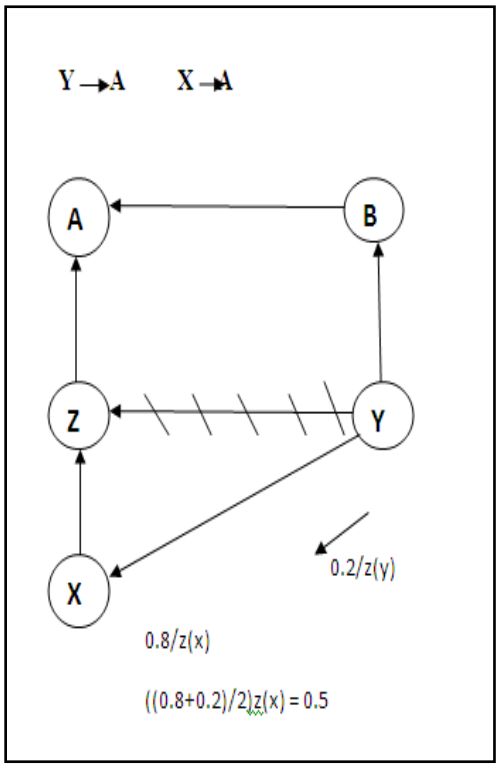

Figure 4: trust values for the node

$T_{mean} = T_{node1} + T_{node2…..}$

$T_x = (0.8 + 0.2)/2$

0.5>0.3

The node ‘X’ will pass the information through node ‘Z’ considering it as a trusted entity. The node y will not send information through node ‘Z’, this would let it look for other optimum path to node ‘A’. This method in turn would reduce the chances of faulty considering a node malicious , as there can be seen a situation that node ‘Z’ is transferring the data from ‘X’ as it is higher priority data comparing to data from ‘Y’.So it might be dropping more packet receiving from ‘Y’.

6.4 Recommendations

The nodes behave in a promiscuous manner. The recommended trust values or the opinion based trust values are calculated. The final trust values are calculated by taking out the mean trust value. The node is considered to be malicious if the mean trust value is less than the threshold value. The node is isolated from the network. The behavior and the trust value of the node accounts it for being compromised or trust worthy.

7. RESULTS

We have taken a default scenario file of 5 nodes, in which we have shown the behavior of black hole AODV. We have named that protocol as BlackholeAODV. The generated Trace file and .Tcl file is analysed in NS2 visual tracer, The numeric results for the nodes are received, those numeric results are

shown as follows. The value of node range from (0-4) and the values of packets are in Kilobytes.

Node	Packets sent	received	transferred	forwarded	dropped
0	1587	4676	2954	595	87
1	372	1571	0	43	41
2	1580	4768	60	572	43
3	473	4041	32	791	26
4	1608	4963	56	634	42

Table1: The packet information of 5 nodes

The values from the above table are taken and the corresponding trust values are calculated. The node 4 is found to be malicious, its trust value obtained is less than the threshold trust value(0.3). This node is under black hole attack. The throughput is shown in the form of a graph. The simulation runs for 25 miliseconds, the throughput varies in bytes/second. The throughput for node 1 is as follows.

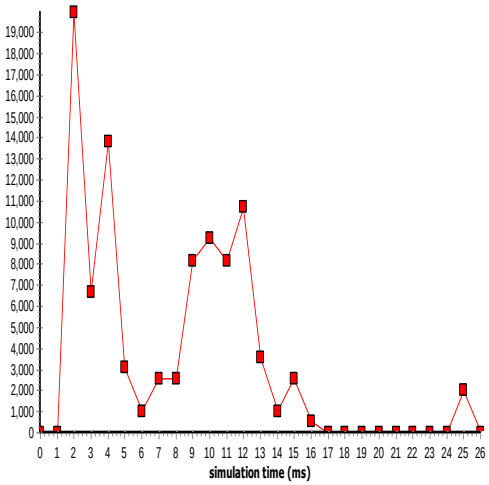

Figure 5: The throughput of the malicious node(trust value<0.3).

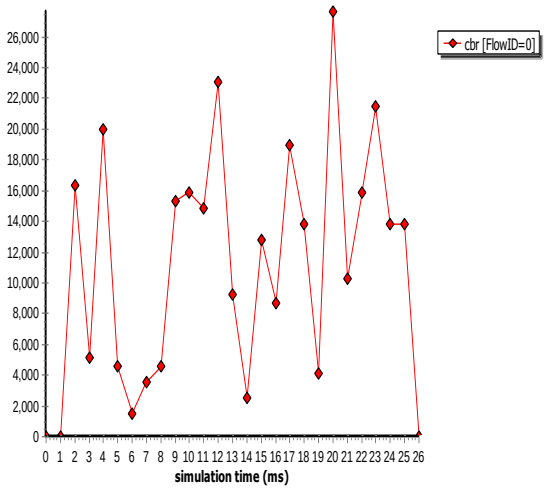

Figure 6: The throughput over a period of 25 ms for a trustworthy node.

8. CONCLUSIONS AND FUTURE WORK

In this paper, the authenticationof the nodes before participating in the network, will allow only authentic nodes to become a part of a network. The trust for individual node has been calculated. The average trust value for the node is calculated. If the averaged trust value is less than the threshold value, then the node is considered to be malicious else it is considered to be trustworthy. The ddifferent phases of trust evaluation in the network will enhance the security in MANETs.

9. REFERENCES

[1] KannanGovindan,PrasantMohapatra," Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey"

[2] Xia Li, Jill Slay ,Shaokai Yu " Evaluating Trust in Mobile Ad Hoc Networks"

[3] MV Raghavendiran N, M Aaqib M, Vijayan R "An approach for detection of malicious node using fuzzy based trust levels in MANET"

[4] D. F. Macedo, A. L. Santos, J. M. S. Nogueira, and G. Pujolle, "A distributed information repository for autonomic context-aware manets,"*IEEE Trans. Netw. Service Management*, vol. 6, no. 1, pp. 45-55, Mar. 2009.

[5] Nagi, E.C.H., M.R. Lyu, and R.T. Chin. "An Authentication Service Against Dishonest Users in Mobile Ad Hoc Networks". in Proceedings of 2004 IEEE Aerospace Conference. 2004. Big Sky, MT, United States: IEEE.

[6] Beth, T., M. Borcherding, and B. Klein. Valuation of Trust in Open Networks.in 3rd European Symposium on Research in Computer Security (ESORICS '94). 1994. Brighton, UK: Springer Verlag.

[7] Pirzada, A.A. and C. McDonald. Trusted Route Discovery with TORA Protocol.in the Second Annual

Conference on Communication Networks and Services Research (CNSR'04). 2004. Fredericton, N.B., Canada: IEEE.

[8] Levien, R. and A. Aiken. "Attack-resistant trust metrics for public key certification".Pro-ceedings of the Seventh USENIX Security Symposium. 1998. San Antonio, TX, USA: USENIX Association.

[9] Zimmermann, P.R., The Official PGP User's Guide. 1995: MIT Press.

[10] Herzberg, A., Y. Mass, and J. Michaeli. Access control meets public key infrastructure, or: assigning roles to strangers. in Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. 2000. Berkeley, CA, USA: IEEE.

[11] Manchala, D.W. Trust Metrics, Models and Protocols for Electronic Commerce Transac-tions.in Proceedings. 18th International Conference on Distributed Computing Systems (Cat.No.98CB36183). 1998. Los Alamitos, CA, USA: IEEE Computer Society.

[12] Manchala, D.W., E-commerce trust metrics and models.IEEE Internet Computing, IEEE 2000. 4(n2): p. p 36-44.

[13] Pirzada, A.A. and C. McDonald. Establishing trust in pure ad-hoc networks.in Proceedings of the 27th conference on Australasian computer science. 2004. Dunedin, New Zealand: Australian Computer Society.

[14] Virendra, M., et al. Quantifying Trust in Mobile Ad-Hoc Networks. in International Con-ference on Integration of Knowledge Intensive Multi-Agent Systems, 2005 (KIMAS '05). 2005. Waltham, Massachusetts, USA: IEEE.

[15] Charles E. Perkins,Elizabeth M. Royer " Ad-hoc On-Demand Distance Vector Routing"WASA, 2006, pp. 695-710.

[16] A.PravinRenold, R.Parthasarathy" Source based Trusted AODV Routing Protocol for Mobile Ad hoc Networks" ICACCI 12 Proceedings of the International Conference on Advances in Computing, Communications and Informatics. Pp-1271-1275

[17] F.Thachil, KC Shet" A trust based approach for AODV protocol to mitigate black hole attack in MANET" 2012 International Conference on Computing Sciences.

[18] Poonam, K.Garg, M.Misra" Misbehaving Nodes Detection Through Opinion Based Trust Evaluation Model in MANETs" International Conference and Workshop on Emerging Trends in Technology(ICWET 2011)- TCET Mumbai

[19] WenjingLou,Wei Liu YuguangFang"SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks" IEEE INFOCOM 2004